ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue II, February 2018

Security Attacks in Adhoc Wireless Networks: A Survey

Nami Susan Kurian

Assistant Professor, Electronics and Communication Engineering, Rajalakshmi Institute of Technology, Chennai, India

***Abstract*— Security has become the most challenging issue in network management and implementation. Adhoc wireless networks play a vital role in all real time emergency applications. One of the primary issues that adhoc network faces nowadays is protection from serious attacks. Network size has grown and issues have increased. If the security is compromised, there could be serious consequences starting from stealing of information, loss of privacy to failure of complete network. Adhoc networks are influenced to a wide range of attacks compared to wired and infrastructure based network due to its unique characteristics. In this paper, we throw light on the security requirements, in-house and outdoor security threats and mechanism used to overcome such security issues in adhoc wireless network. We also confer in detail about layer wise attacks in Adhoc networks.**

***Index Terms*— Adhoc networks, Security, Attacks, Security issues, Threats**

I. INTRODUCTION

Adhoc networks are dynamically formed network without the use of existing network or without the use of a centralized management. Nodes are communicated through radio waves. The entire network is distributed and nodes are connected without any access points or base station.

Wireless Network architecture can be classified into two different types – Infrastructure based and Infrastructure less networks[1]. In case of infrastructure based network, nodes are connected with physical representation. Some examples for these kinds of networks are GSM, UMTS and WLAN etc. Second is infrastructure less network where the node is communicated without any fixed physical representation (without BS). As there is no centralized structure, the nodes in the ad hoc network acts as router (finding path) to send and receive the data. Due to the dynamic nature, ad hoc make the network more robustness.

The importance of adhoc network is highlighted in many fields including military area, provisional level, personal area network, industry sector, bluetooth...etc [6]. One of the most important advantages of adhoc network is that these nodes are self configurable and self healing.

Fig. 1. Infrastructure-based network

Fig. 2. Adhoc network

II. CHALLENGES IN ADHOC NETWORK

The challenges in designing the transport layer of adhoc network are listed below[3]:

A. Induced traffic

A wireless network undergoes multihop radio relaying. Link level transmission affects the neighboring nodes of both sender and receiver. Induced traffic in the network is due to the broadcast environment of the channel.

B. Induced throughput unfairness

Unfairness at the transport layer is due to the unfairness at the lower layers like the MAC layer and network layer. The network experience throughput unfairness when an adhoc network uses WLAN-DCF as MAC protocol.

C. Separation of congestion control, flow control and reliability

The transport layer design should be carried out in such a way that adhoc network should be capable of performing congestion control, flow control and reliability separately. Reliability and flow control are end-to-end activities. Congestion can occurs at any point f transmission. There are

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue II, February 2018

number of congestion control mechanisms put forward to avoid loss of packets through congestion.

D. Power and bandwidth constraints

The two important resources of nodes in adhoc networks are: (a) power source (b) bandwidth. The performance of the transport layer is dependent on these two factors. All nodes are battery powered and efficient use of available energy is highly required. Bandwidth is one of the most important constraints in wireless network as the RF spectrum availability is very less.

E. Misinterpretation of congestion

Packet loss and retransmission time out are the two traditional mechanisms used for detecting congestion. There mechanisms are not appropriate for adhoc networks. The reasons are:
– high error rate of wireless channel
–location dependent contention
–hidden terminal problem
–exposed terminal problem
–path breaks
–node failure
–packet collisions

F. Dynamic topology

Due to the mobility of the nodes, there is a rapid change in the topology of adhoc network. This may lead to recurrent path breaks, partitioning and remerging of network and high delay in restoration of paths. Change in network topology affects the performance of transport layer.

III. Types Of Attack In Adhoc Networks

The attacks [2] in WSN can be classified into three different types:
(a) Passive Attacks
(b)Active attacks

Passive Attacks:

A passive attack [5] does not disrupt the operation of the network. The challenger snoops the data in the network without altering it. Detection of passive attack is very challenging as the network does not get affected. One of the best mechanisms to avoid passive attack is to perform encryption on the data being transmitted.

Active attacks:

An active attack [8] attempts to alter the data transmitted over the network and the normal functioning of the network itself will be troubled. There are two types of active attacks – (a) Internal attack (b) External attack
Internal attacks are carried out by nodes within the network and those nodes are called compromised nodes. External attacks are carried out by nodes outside the network. Internal attacks are difficult to prevent as it is been done by nodes within the network.

TABLE I: Classification Of Security Attacks

SECURITY ATTACKS	
Active Attacks	**Passive Attacks**
- Snooping	**MAC layer attacks** (a) Jamming
	Network layer attacks (a)Wormhome attack (b)Blackhole attack (c)Byzantine attack (d)Information disclosure (e)Resource consumption attack (f)Routing attacks
	Transport layer attacks (a)Session hijacking
	Application layer attacks (a) Repudiation
	Other attacks (a)Denial of service (b)Impersonation (c)Manipulation of network traffic (d)Device tampering

ACTIVE ATTACKS:
Snooping:
Snooping is defined as the unauthorized access to another node's data.

PASSIVE ATTACKS

A. Physical and MAC layer attacks

The physical layer deals with the specification of frequency bands. It is also responsible for frequency selection, carrier frequency generation, modulation, signal detection, and data encryption**.** Wireless communication is broadcast [4] by nature and a common radio signal is easy to jam or intercept. An attacker could eavesdrop or interrupt the service of a wireless network physically.

Nodes in WSNs may be deployed in aggressive or insecure environments where an attacker can physically access the network.

Jamming:
Jamming is caused due to interference with the radio frequencies of the network's devices. It is different from normal radio propagation mechanism as it is unwanted and disruptive signal resulting in denial-of-service conditions. A jammer is powerful enough to disrupt the entire network.

B. Network layer attacks

a. Wormhole attack:

In this attack, tunneling of information from one location of the network to another location is carried by attacker.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue II, February 2018

Wormhole attack can be initiated easily by the attacker without prior knowledge on the network.

b. Blackhole attack:

In this attack, during the path finding process, a malicious node advertises the node falsely about. the shortest path or the stable routes to the destination node. The intention of the malicious node is to drop the path finding process or to reroute the nodes such that it does not reach the destination node.

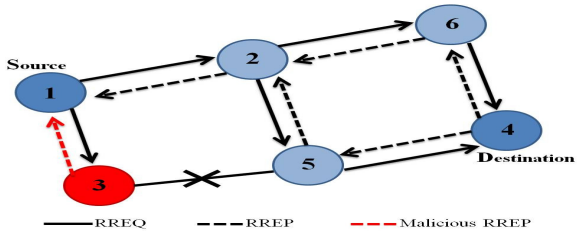

Fig. 3. Blackhole attack

c. Byzantine attack

In this attack, a compromised node or a set of compromised node works in collusion [7]. It carries out attacks such as creating routing loops, routing packets on high drained energy paths and selectively falling packets. It is very hard to find the byzantine attacks in network as the compromised nodes are within the network.

d. Information Disclosure

There is probability of presence of legitimate nodes in the network. A compromised node which is an element of the network may leaks the confidential information to unauthorized nodes in the network.

e. Resource Consumption attack

In this attack, malicious nodes try to waste away the resources of other nodes in the network. These resources include bandwidth, battery power and computational power. These resources are limited in adhoc networks and have to be utilized efficiently to withstand the lifetime of the nodes. This attack is done by sending continuous control packets, stale packets to the nodes thereby keeping the nodes always in the active state. This type of attack is also called sleep deprivation attack.

f. Routing attacks:

There are number of ways in which routing in the network is affected.

(i)Routing table overflow:

In this type of attack, nodes which are not a part of the network adversary (attacker) advertise routes to authorized nodes in the network. The main objective of this attack is to make the routing table overflow with the unwanted entries. This in turn prevents the creation of new entries to the authorized nodes.

(ii)Routing table poisoning

In this attack, the compromised nodes send fallacious routing updates or modify genuine route update packets send to the uncompromised nodes in the network. Routing table poisoning makes some part of the network inaccessible.

(iii)Packet Replication

In this attack, the adversary nodes replicate false or stale packets. This results in unwanted confusions in the network. It also leads to drain of battery and inefficient use of available bandwidth.

(iv)Route cache poisoning

Route cache contains information regarding the routes that has become a part of it. Here, in route cache poisoning, an adversary node poison the route cache.

(v)Rushing attack

During the route recovery process, sender sends the Route Request packet to all neighboring nodes. Upon receiving the RRQ packet, adversary node floods it throughout the network before it gets forwarded by other nodes. The node that gets legitimate RRQ assumes those packets as duplicate packets and discards it. Any route discovered by the source node contains the adversary node and it is difficult to identify the attacker node in case of rushing attack.

C. Transport layer attacks

Session Hijacking:

Once the session between the nodes is conventional, the attacker node acts/masquerades as one of the end nodes in the session and hijacks the session such that the confidential information are leaked.

D. Application Layer Attacks

Repudiation:

It refers to the denial or attempted denial by a node involved in the communication.

E. Other attacks

a. Multi layer attacks

These are the attacks that occur in any layer in the network. Some serious multilayer attacks are as follows:

Denial of Service (DoS) attack:

DoS attack is defined as an event that diminishes or attempts to reduce a network's capacity to perform its expected function. In this type of attack, the authorized nodes are prevented by the unauthorized nodes (advisory nodes) from use of services offered by the network. DoS is carried out in number of ways. One classic way of performing DoS is flooding, flood packets to an access point used in the network

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue II, February 2018

such that the network will not function in the same way as it is designed. So, QoS [11] cannot be guaranteed to the authorized nodes in the network.

SYN flooding:

In this attack, an adversary sends numerous number of SYN packets to the victim node (authorized node). On receiving the SYN packets, an acknowledgement (SYN-ACK) is send back by the victim node. Spoofing of the return address is done by adversary node. In return, a half open connection is established. The victim node updates the table. But the size of the table is limited and hence increased number of half open connections results in overflow of the table.

Distributed DoS attack (DDoS):

This attack is more dangerous than that of DoS attack. In this attack, the network consists of many adversaries and these adversaries prevent the authorized nodes from accessing the resources.

Impersonization:

In this attack, an adversary node masquerade itself as an authorized node. This is done to prevent the authorized nodes in using guaranteed services, injecting false information or to disturb or destroy the network.

IV. Secure Routing In Adhoc Networks

In order to avoid security attacks, secure- routing protocols [9] [10] are designed. Some of the important requirements of secure-routing protocols are (a) detection of malicious nodes (b) guarantee of correct node delivery (c) confidentiality (d) stability against attacks.

Some of the routing protocols designed are :

-Secure –aware Ad-hoc routing protocol (SAR)
-Secure Efficient Distance Vector routing protocol
-Authenticated routing for Adhoc networks (ARAN)
-Security aware AODV networks

V. Conclusion

The drastic developments in the area of adhoc network help the nodes in forming self-configuring, self-healing, self-administering wireless network. Security is now becoming main anxiety in adhoc networks. There are numerous types of attacks discussed in this paper and there are many secure routing algorithms also. Routing algorithms have to be designed in such away to prevent the attacks by taking into consideration of limited resources like bandwidth and battery life. This paper gives insight on the different types of attacks and also highlights the different secure routing protocols to overcome the attacks.

References

[1] Ram Kishore Singh, Padma Nand, "Literature Review of Routing Attacks in MANET", Computing, Communication and Automation (ICCCA), 2016 International Conference," January 2017.

[2] Inderpreet Kaur, A. L. N. Rao, "A Framework to improve the Network Security with Less Mobility in MANET," *International Journal of Computer Applications* (0975 – 8887) Volume 167 – No.10, June 2017.

[3] D. Helen* and D. Arivazhagan, "Applications, Advantages and Challenges of Ad Hoc Networks," *Journal of Academia and Industrial Research,* Vol. 2, Issue 8, January 2014, pp.453-457

[4] Teodor-Grigore Lupuc, "Main Types of Attacks in Wireless Sensor Networks," *Recent Advances in Signals and Systems, pp. 180-186.*

[5] Er. Nitin Aggarwal, Ms. Kanta Dhankhar," Attacks on Mobile Adhoc Networks: A Survey", *International Journal of Research in Advent Technology*, Vol.2, No.5, May 2014

[6] L Raja, S Santhosh Baboo, "An Overview of MANET: Applications, Attacks and Challenges," *International Journal of Computer Science and Mobile Computing*, Vol.3 Issue.1, January- 2014, pg. 408-417.

[7] Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah, " Security challenges in mobile ad hoc networks: a survey," *International Journal of Computer Science & Engineering Survey (IJCSES),* Vol.6, No.1, February 2015.

[8] Jasleen Kaur, Shakti Nagpal," Review Paper on Security Challenges and Attacks in Mobile Ad-Hoc Networks," *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 5, May 2014.

[9] Nami Susan Kurian, Priya B," EMBHMAC:An efficient Multihop broadcast based hybrid MAC protocol for Wireless sensor networks" *Computer Communication and Systems, 2014 International Conference.*

[10] Ankit Mehto, Hitesh Gupta," A Review: Attacks and Its Solution over Mobile Ad-Hoc Network," *International Journal of Engineering Trends and Technology (IJETT)* – Volume 4 Issue 5- May 2013.

[11] Manoj Kumar Khinchi, Dr. Bharat Bhushan," Investigation on MANET Routing Protocols and Quality of Services Management Issues," *International Research Journal of Engineering and Technology (IRJET)*, Volume: 03 Issue: 04, Apr-2016.

Ms. Nami Susan Kurian was born in India in 1989. She completed her B.E in Electronics and Communication Engineering, RGCE, Anna University, Chennai, India. She completed her M.E in Communication Systems, REC, Anna University, Chennai. She is currently working as an Assistant Professor in Rajalakshmi Institute of Technology, Chennai. Her primary area of research is in WSN and MANET.